UNMEDIATED TALK UNDER INCOMPLETE INFORMATION*

Amparo Urbano and José E. Vila**

WP-AD 99-07

Correspondence to A. Urbano: Universitat de València. Facultad de Ciencias Económicas y Empresariales.

Departamento de Análisis Económico. Campus de los Naranjos. Edificio departamental oriental.

46022 Valencia (Spain). Fax: + 34963828249 Phone: + 34963828246 E-mail: amparo.urbano@uv.es

Editor: Instituto Valenciano de Investigaciones Económicas, s.a.
First Edition May 1999
ISBN: 84-482-2122-2
Depósito Legal: V-2102-1999

---

*We want to thank partial support by DGICYT under project PB95-1074. We also thank the comments an and suggestions of participants of the Eighth International Conference of Game Theory (Stony Brook, July 1997) and the XXII Simposio de Análisis Económico (Barcelona, December 1997). The usual disclaimer applies.

** A. Urbano and J.E. Vila: University of Valencia.

UNMEDIATED TALK UNDER INCOMPLETE INFORMATION

Amparo Urbano and José E. Vila

A B S T R A C T

We show the role of unmediated plain conversation as both an information transmission and a coordination device for the class of two-player incomplete information games. Concretely, we prove that any communication equilibrium payoff of such games can be reached as a Nash equilibrium payoff of the game extended by a two phase (exante and interim) unmediated communication protocol. This protocol is constructed by using communicative one-way functions, which are, in turn, designed with the help of modern cryptographic tools. A familiar context in which our results could be applied is bilateral trading with incomplete information.

JEL classification number: C72

Key words: unmediated communication, correlated equilibrium.

1 Introduction.

We analyze communication among rational agents in strategic situations. Agents may use communication to coordinate their actions, to transmit information, to signal to make threats and promises and so on. There are various ways in which communication can occur. For instance, agents may use external 'mechanisms' or mediators to communicate: this is referred to as 'mediated talk'; alternatively, they may communicate by just 'talking': by 'plain conversation' or 'unmediated talk'. Our purpose is to analyze whether plain conversation can achieve the same outcome than a communication device.

In a mediated talk, each agent transmits a private message to the mediator who, in turn, produces announcements (private or public) which depend on the individual private messages. Lehrer (1996) constructs a mediated talk where the mediator's announcement is public and agents are allowed to communicate for a long time. He shows that in a complete information game, unbounded (without limit) mediated talk can generate any correlated equilibrium distribution (Aumann, 1974). Lehrer and Sorin (1997) simplify the above mechanism to cover the case of one-shot communication phase and they generalize it to incomplete information. They show that in this last case every communication equilibrium distribution (Forges, 1986) can be generated by a mediated talk[1].

Unmediated talk only considers those mechanisms - procedures to exchange information and to coordinate decisions - where no external device is needed. All communication goes directly from one agent to another. This is usually referred to as cheap talk. Cheap talk is formally defined as pre-play communication that is free: it costs nothing. The final outcome and the participants' payoffs depend only on what they do - their actions - and not on what they say. Models of (non-cooperative) games with complete information where the communication process has been explicitly modeled and included as a pre-play stage in which players exchange messages - in some specific way - before strictly playing[2] are Barany (1992), Aumann and

[1]The main idea of the construction of a mediated talk is to use a finite collection of jointly controlled lotteries. All of them but one remain latent. The active device is selected by the profile of private inputs

[2]These is another approach which does not model the process by which players ex-

Hart (1993), Gossner (1997) and Urbano and Vila (1997). Barany shows that, if there are at least four players, any correlated equilibrium of a normal form game with complete information coincides with a Nash equilibrium of an extended game in which the players engage in costless conversation (cheap talk before they play the strategic-form game in question). However, under this scheme of conversation - protocol - if there are only two players then the set of Nash equilibria with cheap talk coincides with the subset of correlated equilibria induced by perfectly correlated signals, i. e. publicly observed randomized devices. Aumann and Hart define 'polite talk' as that talk that allows players to talk one at a time and show that by means of it players can get the bi-span[3] of the Nash equilibria of the original game. Gossner examines how information stems from communication, therefore linking communication mechanisms and information structures. Finally, Urbano and Vila extend Barany's results to the class of two player games of complete information by constructing an unmediated communication encryption scheme with private key which is based on computing exponential functions over finite fields[4].

For games of incomplete information, Forges (1990) extends the result of Barany. She constructs a scheme of plain conversation which is a universal mechanism for all noncooperative games with incomplete information and at least *four players*[5]. In particular, she shows that every solution that can be achieved by means of an arbitrary communication mechanism - a procedure

change messages and 'reasonable' arguments justify properties that we may expect from communication: see for instance Rabin (1990, 1993), Farrell (1987, 1988), Farrell and Rabin (1996) and Hurkens (1996) among others.

[3]The bi - span of a set $A \subseteq R^2$ is defined as follow: it is the set of all vectors $(x,y) \in R^2$ for which there exists a bounded martingale $\{(X_n, Y_n)\}_{n=1,2,...}$ with values in R^2 that starts at (x,y) (i. e. $(X_1, Y_1) = (x,y)$); it converges to A (i. e. $(X_n, Y_n) \longrightarrow (X_\infty, Y_\infty) \in A$ almost surely); and finally it satisfies the 'bi' property that for each n either $x_{n+1} = x_n$ a.s. or $y_n = y_{n+1}$ a.s.. Thus, at each stage of the martingale, either the X-coordinate stays constant (and the Y-coordinate 'splits'), or the Y-coordinate is constant (and the X-coordinate 'splits'). Note that if one drops the 'bi' requirement, then the resulting set is precisely the convex hull of A.

[4]See Pohling and Hellman (1978), River, Shamir and Adleman (1978). The enciphering and deciphering transformations are based on Euler's generalization of Fermat's theorem. The security of the scheme rest on the complexity of computing discrete logarithms in the Galois fields. This is like a one-way function which is easy to compute but hard to invert.

[5]If the requirement of finite message sets is relaxed, the result holds also for the three player case. See Forges (1990).

helping the players to exchange information and to coordinate decisions - is a correlated equilibrium payoff of the game extended by the scheme of plain conversation[6] and by Barany's construction a similar result holds also with the Nash equilibrium concept. The scheme of plain conversation is universal because it does not depend on the specifications of the game, nor on the solution to achieve. Also, Aumann and Hart extend their results to the case of one-side incomplete information and show that the equilibrium involves the informed player 1 revealing some of his information, as well as both of them performing joint randomization. Mor Amitai (1996) extends the above model to incomplete information on both sides.

We construct a scheme of unmediated communication (with finite message sets) which is a universal mechanism for all normal-form two-players games with incomplete information , thus solving Forges (1990) and Barany's open problem. Our approach follows that of Urbano and Vila (1997,1998) with public messages but private meaning. This approach is closely related to the one used to model 'oblivious transfers'[7] and those used to solve problems such that 'coin flipping by phone' (Blumm, 1981) or 'playing Mental Poker with no real cards' (Rabin, 1981)[8].

However, these public and private characteristics of messages have to be related in some specific way in order to control the integrity of the whole exchange of information. Thus we have to use ciphers with some properties, in particular, that they commute among them. The use of commutative ciphers is also appealing by their 'fairness' and 'usefulness' in games where players

[6]The corresponding equilibrium strategies use only finite set of messages.

[7]An oblivious transfer is a probabilistic information exchange such that both the sender and the receiver cannot be sure of the real meaning of the message.

[8]In the 'coin flipping by phone', the problem is to devise a scheme whereby a player, say Bob, can call heads or tails and the other, say Alice, can flip in such way that each has a 50% chance of winning. Flipping a real coin over the phone is clearly unsatisfactory because if Bob call 'heads', Alice can simply say 'Sorry, tails'.

Mental poker is played like ordinary poker but without cards and without real verbal communication; all exchange between the players must be accomplished using messages. It may perhaps make the ground rules clearer if we imagine two players, Bob and Alice again, who want to play poker over the telephone. Since it is impossible to send playing cards over a phone line, the entire game (including the deal) must be realized using only spoken (or digitally transmitted) messages between the two players. Obviously any player may try to cheat. A fair method of playing Mental Poker should preclude any sort of cheating.

may cheat as the ones mentioned above. However, the main problem with this approach is that it is very difficult to build up commutative ciphering and deciphering functions in general spaces. In this paper we solve this problem by using exponential ciphers over a finite Galois field of prime order p (p a prime number). Thus, we construct[9] a communication encryption scheme with private key, which is based on computing exponential functions over a finite field.

We assume that the pre-play communication phase is finite and that the player have bounded calculation skills[10], i.e. they need a non-null period of time to make any calculation[11]. Also a technical assumption, shared with Barany, Forges and Urbano and Vila is needed: the payoffs of the game must be rational.[12].

We will show that our scheme is self-enforcing, in the sense that no player wants to deviate from it if the other does not, and that it implements any communication as a Nash equilibrium of the game extended by two stages (ex-ante and interim) of pre-play communication.

To the best of our knowledge, the only application of modern cryptography to game theory, apart from Urbano and Vila (1997,1998) is Gossner (1998). He does not rely on a particular protocol but rather on the fundamental[13] and unproved theoretical assumption of the existence of a

[9]Alternative constructions to ours are those based on pseudorandom generators. A pseudorandom generator is a deterministic algorithm expanding short random seeds into much longer bit sequences which 'appear' to be random (although they are not).

[10]Constructions of secure encryption schemes are based on various intractability assumptions. Classical cryptography assumes that two agents, say A and B, share some secret information before they start to exchange messages, while another agent, say C, tries to spy them. In modern cryptography, A and B share no secret information before they communicate. In typical modern cryptosystems, messages are sent from A to B using some keys. Why C cannot replicate the above agents computations?. Here intervenes the boundedness of agent's rationality. All the computations needed by A and B can be done in reasonable time, whereas that of C would need ages. Also, this distinction between computations that can be implemented in relatively short time and computations which are intractable may be modeled by polynomial and unpolynomial Turing machines.

[11]This time can be as short as we want.

[12]This assumption is needed to replicate some probability distributions by choosing a message uniformly at random from a finite set. Anyway this assumption is not a limitation since it is always possible to approximate a real parameter by a rational one.

[13]A major tool in the construction of cryptographic protocols is the concept of 'zero

trapdoor function. Assuming that players are represented by Turing machines, Gossner obtains a 'Folk Theorem' in which the usual minmax level in mixed strategies is replaced by the minmax in correlated strategies.

A familiar economic application which has been widely analyzed under communication is that of *bilateral trading with asymmetric information*. In particular, the simplest model of trade which involves one seller and one buyer, who both privately know their own value for a single object initially owned by the former agent. The sealed bid double auction mechanism has been extensively used to solve this simple collective choice problem[14]. As observed by many authors it is usually impossible to prevent traders from communicating in non-binding unmediated way before making decisions. Thus, if communication is performed without the help of a mediator, the pre-play phase really represents the (unbinding) negotiation between traders. Matthews and Postlewaite (1989) have proved that the outcomes of a large class of trading mechanisms could be achieved as Nash equilibria of the double auction game preceded by pre-play communication[15].

The fact that unmediated pre-play communication enables the traders to reach a large class of outcomes is a desirable property, because it implies that traders can dispense with a planner[16].

The plan of the paper is as follows: In section 2 some notation and basic

knowledge' proofs systems, and the fact that they exist for all languages in NP (provided that one -way functions exist). Loosely speaking, zero-knowledge proofs yield nothing but the validity of the assertion. They provide a tool for 'forcing' parties to follow a given protocol properly. We thank S. Hart for pointing us this remark.

[14]See, for instance, Chatterjee and Samuelson (1983), Gresik (1996), Leininger, Linhart and Radner (1989), Matthews and Postlewaite (1989) among others. Of course, more general trading mechanisms have also been proposed. See Forges (1990), Myerson and Sattethwaite (1983)...

[15]Forges (1998) extends the above approach to the case of several buyers. By relying on a general revelation principle she obtains a simple description of all equilibria which can be achieved by allowing (ex-ante and interim) pre-play communication in the contracting game (i. e. the game which represents the last stage of a negotiation process between the traders and reduces to the δ-sealed-bid auction in the two player case).

[16]However, as emphasized by Matthews and Postlewaite (1989) and Palfrey and Srivastava (1991), pre-play communication dramatically worsens the full implementation problem. The last authors solve this issue in the case of independent types and private values by designing for any interim efficient allocation, a pre-play communication proof mechanism, which uniquely implements this allocation. However, it is not universal

concepts are set up. Some useful key points of Number Theory are refreshed in section 3. The main result and the communication protocol are presented in section 4. Section 5 analyzes some examples, while section 6 is devoted to show the properties of the communication protocol and the characterization of the distributions induced by deviations. In section 7 we cover the way from correlated to Nash equilibrium. The main result is proved in section 8. Finally, section 9 concludes.

2 Definitions and concepts.

Let us consider a two-person game G with incomplete information. Following Harsany, such a game can be described by

1. A set of 2 players
2. Finite sets K_h, $K_{h'}$ $(h, h' = 1, 2,\ h \neq h')$ of states of private information or types of each player with $K_h = \{k_h^1, ..., k_h^v\}$ and $K_{h'} = \{k_{h'}^1, ..., k_{h'}^r\}$.
3. A probability distribution π over $K = K_1 \times K_2$
4. Finite sets A_h, $A_{h'}$ $(h, h' = 1, 2,\ h \neq h')$ of actions of each player with $A_h = \{a_h^1, ..., a_h^s\}$ and $A_{h'} = \{a_{h'}^1, ..., a_{h'}^t\}$.
5. A payoff function u_h for each player $(h = 1, 2)$ over $K \times A$ on R (or Q when specified so, as in the propositions below) where $A = A_1 \times A_2$

G is played in the following way: firstly, nature chooses an element of K according to π and communicates each player his corresponding component. Secondly, both players move simultaneously and each player receives the payoff given by his function u_h that depends on types and actions.

We allow the players to communicate before simultaneously choosing their actions. This pre-play communication can be performed with the help of a mediator which receives private signals from the players and sends private announcements to them. We model this mediator or 'communication device' as follows:*a communication device for G is a collection $d = \{I_h, O_h, q\}$ where I_h is a set of inputs from player h, O_h is a set of outputs to player h and q is a transition probability that chooses the outputs in $O_1 \times O_2$ as a function of the inputs of $I_1 \times I_2$.*

Once this device d is defined, we can construct from G an extended game G_d with the following steps:

1. Nature chooses a vector of players' types according to π and informs each player of its own type
2. Each player transmits an element of I_h to the device
3. The device selects an output vector according to q and informs each player of his own output
4. Each player takes an action in A_h and payoffs are given by the payoff functions

A communication equilibrium of G is a Nash equilibrium of the game extended by adding one of these communication devices.

We say that a communication device is canonical if $I_h = K_h$ and $O_h = A_h$, $\forall h = 1, 2$. A canonical communication equilibrium of G is a Nash equilibrium of a extension of this basic game G by a canonical communication device. We can assume that, in such an equilibrium, both players have incentives to tell the device the truth and to obey its suggestions faithfully. The revelation principle shows that any payoff that can be reached by a communication equilibrium can also be gotten by a canonical communication equilibrium.

When the sets of inputs of a (canonical) communication device are singletons, we call it a (canonical) correlation device. The (canonical) correlated equilibria of a game are the Nash equilibria of the extensions of this game by any (canonical) correlation device.

Let us remark that in a canonical communication equilibrium, the associated transition probability is a distribution over A conditional to the types in K. A logical question that arises at this point is: Which are the properties that an arbitrary conditional distribution q must satisfy in order to be a communication equilibrium distribution?. These conditions are given by a system of linear inequalities, as we can see in Forges (1990). In order to write them, we need to derive the probability distribution that resumes the knowledge of player h of type k_h^l when he has declared to be of type $k_h^{l'}$. This distribution over

$$K_{h'} \times A_h \times A_{h'} = \{k_{h'}^1, ..., k_{h'}^r\} \times \{a_h^1, ..., a_h^s\} \times \{a_{h'}^1, ..., a_{h'}^t\}$$

$(h \neq h')$ is given by:

$$\Delta_h^{ll'}(k_{h'}^m, a_h^i, a_{h'}^j) = \pi(k_{h'}^m | k_h^l) q(a_h^i, a_{h'}^j | k_h^{l'}, k_{h'}^m)$$

The communication equilibrium conditions formalizes the following intuition: once players know their own types, the interim expected payoff obtained by telling the truth and by obeying the suggestion is the highest payoff that they can obtain. Hence, $\forall k_h^l, k_h^{l'} \in K_h$:

$$\sum_{m=1}^{r} \sum_{i=1}^{s} \sum_{j=1}^{t} \Delta_h^{ll}(k_{h'}^m, a_h^i, a_{h'}^j) u_h(k_h^l, k_{h'}^m, a_h^i, a_{h'}^j) \geq$$

$$\sum_{i=1}^{s} \Delta_h^{ll'}(a_h^i) max_{a_h \in A_h} \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_h^{ll'}(k_{h'}^m, a_{h'}^j | a_h^i) u_h(k_h^l, k_{h'}^m, a_h, a_{h'}^j)$$

where $\Delta_h^{ll'}(a_h^i) = \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_h^{ll'}(k_{h'}^m, a_{h'}^j, a_h^i)$ denotes the marginal distribution on P_h's actions and

$$\Delta_h^{ll'}(k_{h'}^m, a_{h'}^j | a_h^i) = \frac{\Delta_h^{ll'}(k_{h'}^m, a_{h'}^j, a_h^i)}{\Delta_h^{ll'}(a_h^i)}$$

is the conditional distribution on $P_{h'}$'s actions and types, given that P_h is suggested to play a_h^i. In other words, we have that, $\forall\ \hat{a}_h^i \in A_h$:

$$\sum_{m=1}^{r} \sum_{i=1}^{s} \sum_{j=1}^{t} \Delta_h^{ll}(k_{h'}^m, a_h^i, a_{h'}^j) u_h(k_h^l, k_{h'}^m, a_h^i, a_{h'}^j) \geq$$

$$\sum_{m=1}^{r} \sum_{i=1}^{s} \sum_{j=1}^{t} \Delta_h^{ll'}(k_{h'}^m, a_h^i, a_{h'}^j) u_h(k_h^l, k_{h'}^m, \hat{a}_h^i, a_{h'}^j)$$

Since the set of communication equilibrium distributions is defined by these linear inequalities, we have that it is a convex polyhedron. Moreover,

if the parameters of the original game (payoffs and distributions on types) are rational, all the members of the above inequalities will be in Q and the distributions of the vertices of the polyhedron will be Q-evaluated as well. This fact will be used below.

Forges' example:

Let us consider the deterministic communication equilibrium example of Forges (1990). The game consists of two players with two feasible types, say $K_1 = \{k_1^1, k_1^2\}$ and $K_2 = \{k_2^1, k_2^2\}$ each of them. The sets of actions of players are $A_1 = \{a_1^1, a_1^2, a_1^3\}$ and $A_2 = \{a_2^1, a_2^2\}$ respectively. Assume that the following deterministic rule is associated to a (canonical) communication equilibrium of the original game.

$$\begin{array}{cc} & \begin{array}{cc} k_2^1 & k_2^2 \end{array} \\ \begin{array}{c} k_1^1 \\ k_1^2 \end{array} & \left(\begin{array}{cc} (a_1^1, a_2^1) & (a_1^1, a_2^1) \\ (a_1^1, a_2^1) & (a_1^2, a_2^2) \end{array} \right) \end{array}$$

Notice that if player 1 announces type k_1^2, he gets to know player 2's type but at the same time, player 2 will play an action depending on his own type. However, if player 1 declares type k_1^1, he learns nothing.

Forges [1990] constructed this example in order to show that with a correlation device and her plain conversation scheme, signaling and decision of an action cannot be done simultaneously and one may fear that: player 1 could send information to player 2 as if he were of type k_1^1, so as to induce a_2^1, but would interpret player 2's messages as would type k_1^2, so as to learn player 2's type. Hence, if player 1 of type k_1^2 prefers (a_1^3, a_2^1) to (a_1^2, a_2^2) when P_2 is of type k_2^2 (which is not precluded by the communication equilibrium conditions), he could obtain an extra profit by acting in this way.

This was the motivating example for our protocol. In the sequel, we will show how to avoid the above problem. However, to construct our scheme of communication we need to define first the set of messages and the one-way functions.

3 The set of messages and the ciphering - deciphering functions.

A protocol is an agreed upon procedure according to which players exchange a set of messages. A message is a piece of information transmitted from one player to another.

Thus, in order to construct a communication procedure, both players have to agree first on the space of messages and to associate to every pair of strategies of the original game a pair of messages - a two letter word - from the message space. Notice that since the distribution q is Q-evaluated, it is always possible to associate to every pair of strategies (a_i, b_j) a number of different two letter words such that if one of these words is selected at random uniformly, the probability that it will be associated to the pair (a_i, b_j) is exactly $q(a_i, b_j)$. Once the space of two letter words is constructed, players proceed to exchange messages, i.e. words.

However, since the main problem is that in this process of exchanging messages players have no reason to trust each other, we organize the conversation in such a way that messages are public but with private meaning. Hence, one of the players, say player 1, encodes separately (under a private coding) every letter of all two letter words and sends them to the other player. This second one selects one of the encrypted words without knowing its real meaning, and encodes his corresponding letter and sends it back to the first player.

Note, however, that in order to control the integrity of the whole exchange of information we need to impose some properties on the one-way functions being used. In particular, we need that they commute among them. Commutation allows players to send public messages with private meaning without any loss of efficiency of the real information been transmitted. Thus, they can encode and decode previously encoded messages while keeping privacy and control over the real meaning of them[17]. A nice physical analogy for the above process is the following: we can view encryption as equivalent to placing a padlock on a box containing the message. A player, say Bob, initially locks all the messages in individual indistinguishable boxes with padlocks all

[17] The situation is completely different with the arbitrary permutations used by Barany (1992).

of which have key B. The other player, say Alice, selects a box and then sends it back to him the chosen box to which she has also added her own padlock with key A. Bob removes his padlock from the box and returns to Alice the box still locked with her padlock. Notice the implicit use of commutativity in the order in which padlocks are locked and unlocked.

Hence, to construct the communication protocol we need to use ciphering and deciphering functions with commutative properties as in Urbano and Vila (1997, 1998). As it was said there these functions can be defined by using exponential ciphers in the way proposed by Pohling-Hellman (1978)[18]. This methodology is based on Number Theory. For the sake of completeness we include here some basic concepts of it in order to understand our constructions[19].

Two integers a and b are *Congruent Module* another integer m if and only if $\exists\ k$ integer such that $a - b = km$. Let us denote by $a + mZ$ the set of all integers congruent to a module m. When the integer m is clear from the context, we write $a + mZ = \bar{a}$. Given m, it can be proved that there exist exactly m distinct sets of this kind given by $\bar{0}, \bar{1}, ..., \overline{m-1}$. We write $Z_m = \{\bar{0}, \bar{1}, ..., \overline{m-1}\}$.

Algebraic operations with these sets are performed in a similar way to common integers, i. e. $\bar{a} + \bar{b} = \overline{(a+b)}$ $\bar{a}\bar{b} = \overline{(ab)}$. It can be proved that $(Z_m, +, .)$ is a *commutative ring*. It is easy to see that $\bar{a} \in Z_m$ has an inverse in Z_m if and only if a is prime to m (i.e. the maximum common divisor of a and m is 1). If $\bar{a}$ has inverse it is said that it is a *unit* of the ring Z_m. The number of units of Z_m is then the number of integers lower than m and prime to m. This number is denoted by $\phi(m)$ where ϕ is known as *Euler function* [20]. If $\bar{a}$ is a unit, then $\bar{a}^{-1} = \bar{a}^{\phi(m)-1}$. So, $\bar{a}^{\phi(m)} = \bar{1}$.

Let us consider the ring Z_p with p a prime number. Then, every no null element of Z_p is a unit. The ring Z_p is in fact a finite field of p elements

[18]The existence of one-way functions is still an open problem. The schemes of Pohling and Hellman (1978) and Rivest, Adleman and Shamir (1978) are usually considered as functions with this property. For a more detailed discussion of this topic, see Gossner (1998).

[19]A more complete exposition of them can be found in Vinogradov (1955) and Le Veque (1977)

[20]This function is given by $\phi(m) = \prod_{i=1}^{t} p_i^{m_i - 1}(p_i - 1)$ where $m = p_1^{m_1}...p_t^{m_t}$ is the prime factor decomposition of m.

called Galois Field of order p and denoted by $GF(p)$.

To define the set of basic messages (or 'letters'), both players choose jointly a prime number p *large enough* in a sense that we will make precise later. This set will be given by the units of $GF(p)$ except $\bar{1}$:

$$M = Units\ GF(p) - \{\bar{1}\} = \{\bar{2}, ..., \overline{p-1}\}$$

To define the ciphering and decoding functions of the players, each one of them, P_h, takes secretly and independently two integers e_h, d_h such that

$$(e_h + \phi(p)Z)(d_h + \phi(p)Z) = (1 + \phi(p)Z)$$

where $\phi(p)$ is the Euler function acting over p[21]. These functions are constructed from these numbers in the following way, $\forall \bar{m} \in M$, $E_h(\bar{m}) = \bar{m}^{e_h}$ and $D_h(\bar{m}) = \bar{m}^{d_h}$. It can be proved that:

1. E_h y D_h are inverse. (Since $(e_h + \phi(p)Z)(d_h + \phi(p)Z) = (1 + \phi(p)Z)$ we have that $\exists t \in Z$ such that $e_h d_h = t\phi(p) + 1$. Hence $E_h(D_h(\bar{m})) = \bar{m}^{t\phi(p)+1} = \bar{m}\bar{m}^{\phi(p)^t}$ and because $\bar{m}^{\phi(p)} = \bar{1}$, we can say that $E_h(D_h(\bar{m})) = \bar{m}$. Then the two functions are inverses).

2. The four permutations commute. $(E_h(D_{h'}(\bar{m})) = \bar{m}^{e_h d_{h'}} = \bar{m}^{d_h e_{h'}} = D_h(E_{h'}(\bar{m}))$ and similarly for any other combination.)

3. $\bar{m}$ cannot be calculated by P_h $(h = 1, 2)$ from $E_{h'}(\bar{m})$ and $D_{h'}(\bar{m})$ $(h \neq h')$. In order to break the cipher, P_h needs to know the keys $e_{h'}$ and $d_{h'}$ of player $P_{h'}$. The knowledge of one of these integers allows to ascertain the other, since they are inverses in $Z_{\phi(p)}$. The information that a player has is, in the best of the cases, a list of messages, i.e. $\bar{m}$, and its codification $\bar{m}^{e_{h'}}$. Hence, to break the code used by $P_{h'}$ is the same than to calculate the logarithm in base $\bar{m}$ of $\bar{m}^{e_{h'}}$ in the Galois field $GF(p)$, i.e. $e_h = \log_{\bar{m}}(\bar{m}^{e_{h'}})$. The fact that P_h cannot decipher this key is due to the difficulties of calculating this logarithm[22].

[21] Since p is already a prime integer, we have that $\phi(p) = p - 1$.

[22] This calculation takes $\exp((ln(p)ln(ln(p)))^{\frac{1}{2}})$ steps (See Adleman (1979)). If both players agree on the use of a prime large enough (200 digits, for instance), it would take 1.2×10^{23} steps to calculate it. Even if it is assumed that P_h may use a computer, which

4 Communication scheme.

In this section we formalize the communication scheme. Our goal is to extend any two-player game G with incomplete information and with rational parameters (payoffs and a priori distributions), by an interim plain conversation protocol such that any (canonical) communication equilibrium of G can be obtained as a correlated equilibrium of this extended game:

Theorem (Main result) *Let G be a two-player game with incomplete information and rational parameters. Let $T(G)$ the set of communication equilibrium payoffs of G. Then, every payoff in $T(G)$ is achievable as a correlated equilibrium payoff of the game extended by a universal mechanism of interim plain conversation. The correlated equilibrium strategies only use finite sets of messages.*

With correlated equilibrium as the solution concept restriction to public messages does not prevent players from exchanging private messages. Indeed, before the conversation phase, players may get privately, from a correlation device, codes which they can use to talk safely in public. Also notice that the help a correlated device in the unmediated conversation involved in the main result might be much more informative than the use of a (canonical) communication device. This situation arises since, in the correlated equilibrium, both players must receive all the suggestion for acting and signaling before knowing their types from nature while in the communication equilibrium each players transmits just his type and gets only the action to play. Hence, in the former situation, players might learn from the correlated device how to interpret messages for each of their possible types and they may use it for their own interest. We need, then, a safe way to preclude this kind of 'experimentation' by player h of type k_h^l as if he were of any other type in K_h. To this end we construct a protocol where a player is informed about his action not from the correlation device but from the other player. Since only two player are involved, no checking control can be established to prevent players from cheating when they transmit information. However, the

could make an operation every μseg (i. e. 10^{11} steps a day), he would need 10^{12} days or, in other words, several billions of years to make the above calculation. Thus, it is not possible to ascertain $\bar{m}$ from its codification. This kind of exponential ciphers, jointly with the one proposed by Rivest-Shamir-Adleman (1978), are being applied in real situations where the integrity of the exchanged information is very important (military cryptography, sales through Internet, etc.)

protocol can be designed in such a way that deviations are not profitable for the cheating player (self-enforcing protocol).

In order to communicate, both player are helped by a correlation device *cd*. This device will provide the players with the elements that they need to choose a message according to a given distribution and with *dictionaries* to translate the selected message into suggested actions depending on their own types. To this end, the correlation device performs the following functions:

1. *cd* selects a big prime number p. Let us denote by $M = GF(p) - \{\bar{0}, \bar{1}\}$ the set of message for the communication process.

2. *cd* chooses ν different pairs in $M \times M$, where ν is the lowest common multiple of the denominators of $q(a|k)$, $\forall a \in A, k \in K$. Let V be the set formed by these ν ordered pairs or *two letter words*.

3. *cd* chooses two injective functions $\mu_h : K_h \longrightarrow M$ $(h = 1, 2)$ and two distinct elements $c_h \in M$, $(h = 1, 2)$ such that, $\forall\ l, l', m, m'$:

$$0 \neq \mu_1(k_1^l)^{c_2} + \mu_2(k_2^m)^{c_1} \neq \mu_1(k_1^{l'})^{c_2} + \mu_2(k_2^{m'})^{c_1} \neq 1$$

   Let γ^{lm} be the element of M given by $(\mu_1(k_1^l)^{c_2} + \mu_2(k_2^m)^{c_1})^{c_1 c_2}$. The functions γ_h^{lm}, $(h = 1, 2)$ resume all the information about both players' types.

4. *cd* defines set $V_{a,k}$, $\forall a \in A, k \in K$, *partitions of the message set* such that:

   (a) $Card(V_{a,k}) = q(a|k)\nu$

   (b) $\{V_{a,k} | a \in A\}$ is a partition of V for every $k \in K$

   Let us remark that by choosing an element of V at random uniformly, say (α_1, α_2), we have that:

$$Prob((\alpha_1, \alpha_2) \in V_{a,k}) = q(a|k)$$

   Hence, these partitions of V are emulating the communication equilibrium distribution q.

(a) *cd* constructs *dictionaries or decision sets* A_h^i, for every $a_h^i \in A_h$ in the following way:

$$A_1^i = \{\alpha_1^{\gamma_2^{lm}} | (\alpha_1, \alpha_2) \in V_{(a_1^i, a_2^j),(k_1^l, k_2^m)} \ \forall (k_1^l, k_2^m) \in K\}$$

$$A_2^j = \{\alpha_2^{\gamma_1^{lm}} | (\alpha_1, \alpha_2) \in V_{(a_1^i, a_2^j),(k_1^l, k_2^m)} \ \forall (k_1^l, k_2^m) \in K\}$$

(b) *cd* sends the elements p, V, μ_h, c_h and A_h^i to player h.

Once players have received both the above elements from *cd* and types $(k_1, k_2) \in K$ from nature, they must select commutative private codifying and deciphering function E_h, D_h. Afterwards, the conversation phase begins. This phase consists of the following steps[23]:

Step 1 Player 2 adds a control letter to every word in V. For instance, he could add to any word $(\alpha_1, \alpha_2) \in V$ a third letter $E_2(\alpha_1\alpha_2)$.

Step 2 Player 1 codifies all the three letter words by using his private function

$$(E_1(\alpha_1), E_1(\alpha_2), E_1(E_2(\alpha_1\alpha_2)))$$

and he sends them back to player 2.

Step 3 Player 2 chooses at random an encrypted word in the above set. Suppose that this word is

$$(E_1(\alpha_1^\star), E_1(\alpha_2^\star), E_1(E_2(\alpha_1^\star\alpha_2^\star)))$$

Step 4 Player 2 calculates $E_2(E_1(\alpha_2^\star))$ and he sends it back to player 2.

Step 5 Player 1 calculates $D_1(E_2(E_1(\alpha_2^\star))) = E_2(\alpha_2^\star)$

Step 6 Both players make public their encrypted type, $\mu_1(k_1^l)$ and $\mu_2(k_2^m)$.

Step 7 Player 1 calculates $\mu_2(k_2^m)^{c_1}$ and he makes it public. In the same way, P_2 communicates $\mu_1(k_1^l)^{c_2}$ to P_1.

[23] By symmetry, the roles of player 1 and player 2 can be exchanged.

Step 8 Player 1 calculates $\gamma_1^{lm} = (\mu_1(k_1^l)^{c_2} + \mu_2(k_2^m)^{c_1})^{c_1}$ and he sends it to P_2.

Step 9 Player 2 calculates $\gamma_2^{lm} = (\mu_1(k_1^l)^{c_2} + \mu_2(k_2^m)^{c_1})^{c_2}$ and he makes it public.

Step 10 Player 1 calculates $E_2(\alpha_2^\star)^{\gamma_1^{lm}}$ and player 2 calculates $E_1(\alpha_1^\star)^{\gamma_2^{lm}}$ and they exchange these messages.

Step 11 Each player deciphers its own message, obtaining $(\alpha_1^\star)^{\gamma_2^{lm}}$ (the first player) and $(\alpha_2^\star)^{\gamma_1^{lm}}$ (the second one).

Step 12 Player 1 plays the a_1^i such that $(\alpha_1^\star)^{\gamma_2^{lm}} \in A_1^i$ and player 2 plays the a_2^j such that $(\alpha_2^\star)^{\gamma_1^{lm}} \in A_2^j$.

Notice that the communication protocol has three different blocks:

Steps 1 - 5: selection at random uniformly of a codified word in V.

Steps 6 - 9: construction of the functions γ_h^{lm}, $(h = 1, 2)$, which resume all the information about both players' types.

Steps 10 - 12: information transmission and decision making about the actions to play.

The above steps completely describe both players' actions along the equilibrium path of the communication phase. However a player, say P_1, can deviate from the protocol and P_2 may realize of it with a positive probability. In this case, we have to specify the punishment strategy of P_2. To this end, we assume that P_2 of type k_2^m will follow the mixed strategy $\rho_2^m(a_2^j)$ given by:

$$\rho_2^m(a_2^j) = \frac{1}{|K_1|} \sum_{k_1^l \in K_1} \sum_{a_1^i \in A_1} q(a_1^i, a_2^j | k_1^l, k_2^m)$$

Let us notice that ρ_2^m assigns to each a_2^j a probability that depends neither on the expected type of P_1 nor on the expected action of this last player. Hence, ρ_2^m can be understood as an uncoordinated way of choosing the action a_2^j: the punishment in a protocol is undertaken by breaking its power as both an information transmission and a coordination device.

Let us remark that a player may deviate at steps 6 (by declaring a wrong type), step 7 (by calculating $\mu_h(k_h^l)^{c_{h'}}$ in a wrong way), steps 8 or 10 (by sending a different message) and step 12 (by disobeying the suggestion of the protocol). The effect of each deviation is the following:

Step 6 By declaring $k_h^{l'}$, player h of type k_h^l induces a distribution on actions given by $\Delta_h^{ll'}$ instead of by Δ_h^{ll}.

Step 7 By calculating $\mu_h(k_h^l)^{c_{h'}}$ in a wrong way, P_h just puts some noise into his own information set and he does not affect either the knowledge or the behavior of the other player. Hence, a deviation at this step is not useful.

Steps 8 or 10 By changing the right value of γ_h^{lm} or by sending an element of $GF(p)$ distinct from $E_{h'}(\alpha_{h'}^{\star})^{\gamma^{lm}}$, P_h induces a different distribution $\bar{\Delta}_h^{ll'}$ over $K_{h'} \times A_h \times A_{h'}$. The properties of this new distribution will be analyzed below.

Step 12 At the last step, P_h will play the action that maximizes his expected payoff. Hence, if he receives the suggestion of choosing a_h^i, he will play:

$$\hat{a}_h^i = arg\ max_{a_h \in A_h} \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_h^{ll'}(k_{h'}^m, a_{h'}^j | a_h^i) u_h(k_h^l, k_{h'}^m, a_h, a_{h'}^j)$$

It can be proved that the communication protocol defined above is quasi- sure and self-enforcing, i. e. a player cannot obtain by deviating an expected payoff bigger than that of the communication equilibrium, when the other player obeys faithfully the protocol. Moreover, any deviation of a player can be detected with a probability as close to 1 as we want.

Examples.

Example 1.

Let us apply our communication protocol to an example adapted from Lehrer and Sorin (1996). Consider a two-player games, where player 1, P_1, has two feasible types $K_1 = \{k_1^1, k_1^2\}$ and player 2, P_2, only one,

say $K_2 = \{k_2^1\}$. Suppose that $\{a_1^1, a_1^2\}$ is the set of feasible actions of P_1 and $\{a_2^1, a_2^2\}$ that of P_2. Payoff matrices are given by

$$\begin{array}{cc} & \begin{array}{cc} a_2^1 & a_2^2 \end{array} \\ \begin{array}{c} a_1^1 \\ a_1^2 \end{array} & \left(\begin{array}{cc} (6,6) & (3,8) \\ (7,3) & (0,0) \end{array} \right) \end{array}$$

when P_1 is of type k_1^1 and by

$$\begin{array}{cc} & \begin{array}{cc} a_2^1 & a_2^2 \end{array} \\ \begin{array}{c} a_1^1 \\ a_1^2 \end{array} & \left(\begin{array}{cc} (0,0) & (7,3) \\ (3,8) & (6,6) \end{array} \right) \end{array}$$

when he is of type k_1^2.

It is easy to show that the conditional probability distributions

$$\left(\begin{array}{cc} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & 0 \end{array} \right)$$

when P_1 is of type k_1^1 and

$$\left(\begin{array}{cc} 0 & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} \end{array} \right)$$

when he is k_1^2, are associated to a canonical communication equilibrium of the game. Let us apply our protocol to construct a communication scheme which allows the players to obtain the same interim expected payoff (5.5 for both types of player 1).

Recall that this procedure consists on a correlation device choosing the message set, the one-way functions, the partitions of the message space and the decision sets, followed by a plain conversation phase between the players, where they exchange messages forth and back.

Firstly, we focus on the role of the correlated device, say cd, which performs the following functions:

(a) *cd* selects the prime number 43.

(b) *cd* chooses four different two-letter words in $GF(43)\times GF(43)$. Let us assume that these four words are $V = \{(\bar{2},\bar{3}),(\bar{4},\bar{5}),(\bar{6},\bar{7}),(\bar{8},\bar{9})\}$

(c) *cd* selects the functions μ_h given by $\mu_1(k_1^1) = m_1 \in GF(43)$, $\mu_1(k_1^2) = m_2 \in GF(43)$ and $\mu_2(k_2^1) = n \in GF(43)$, with m_1, m_2 and n three distinct elements of $GF(43)$ with the following property:

$$0 \neq \mu_1(k_1^l)^{c_2} + \mu_2(k_2^1)^{c_1} \neq \mu_1(k_1^{l'})^{c_2} + \mu_2(k_2^1)^{c_1} \neq 1$$

$\forall\ h = 1,2$ and $\forall\ l, l' = 1,2$

(d) *cd* defines *partitions of the message set*, given by:

i. $V_{(a_1^1,a_2^1),(k_1^1,k_2^1)} = \{(\bar{2},\bar{3}),(\bar{4},\bar{5})\}$
ii. $V_{(a_1^1,a_2^2),(k_1^1,k_2^1)} = \{(\bar{6},\bar{7})\}$
iii. $V_{(a_1^2,a_2^1),(k_1^1,k_2^1)} = \{(\bar{8},\bar{9})\}$
iv. $V_{(a_1^2,a_2^2),(k_1^1,k_2^1)} = \emptyset$
v. $V_{(a_1^1,a_2^1),(k_1^2,k_2^1)} = \emptyset$
vi. $V_{(a_1^1,a_2^2),(k_1^2,k_2^1)} = \{(\bar{2},\bar{3})\}$
vii. $V_{(a_1^2,a_2^1),(k_1^2,k_2^1)} = \{(\bar{4},\bar{5})\}$
viii. $V_{(a_1^2,a_2^2),(k_1^2,k_2^1)} = \{(\bar{6},\bar{7}),(\bar{8},\bar{9})\}$

(e) Let $\gamma_h^{lm} = (\mu_1(k_1^l)^{c_2}+\mu_2(k_2^m)^{c_1})^{c_h}$. Recall that these functions summarize information about both player's types. *cd* defines *decision sets* (which will allow players to translate messages into actions) as follows:

i. $A_1^1 = \{\bar{2}^{\gamma_2^{11}}, \bar{4}^{\gamma_2^{11}}, \bar{6}^{\gamma_2^{11}}, \bar{2}^{\gamma_2^{21}}\}$
ii. $A_1^2 = \{\bar{8}^{\gamma_2^{11}}, \bar{4}^{\gamma_2^{21}}, \bar{6}^{\gamma_2^{21}}, \bar{8}^{\gamma_2^{21}}\}$
iii. $A_2^1 = \{\bar{3}^{\gamma_1^{11}}, \bar{5}^{\gamma_1^{11}}, \bar{9}^{\gamma_1^{11}}, \bar{5}^{\gamma_1^{21}}\}$
iv. $A_2^1 = \{\bar{7}^{\gamma_1^{11}}, \bar{3}^{\gamma_1^{21}}, \bar{7}^{\gamma_1^{21}}, \bar{9}^{\gamma_1^{21}}\}$

(f) *cd* sends the elements p, V, μ_h, c_h, A_h^1 and A_h^2 to player h.

Once each player knows these elements and receives his own type from nature the conversation phase starts. Suppose that natures has chosen the types k_1^2 and k_2^1. Then, players select independently codifying and deciphering functions E_h and D_h and the communication phase unfolds in the following steps:

Step 1 Player 2 adds a control letter to every word in V. Hence, he constructs a new set given by $\{(\bar{2},\bar{3},E_2(\bar{6})),(\bar{4},\bar{5},E_2(\bar{20})),(\bar{6},\bar{7},E_2(\bar{42})),(\bar{8},\bar{9},E_2(\bar{72})=E_2(\bar{29}))\}$, and he sends it to player 1.

Step 2 Player 1 codifies all the three letter words of the above set

$$\{(E_1(\bar{2}),E_1(\bar{3}),E_1(E_2(\bar{6}))),(E_1(\bar{4}),E_1(\bar{5}),E_1(E_2(\bar{20}))),$$

$$(E_1(\bar{6}),E_1(\bar{7}),E_1(E_2(\bar{42}))),(E_1(\bar{8}),E_1(\bar{9}),E_1(E_2(\bar{29})))\}$$

and he sends the encrypted words back to P_2.

Step 3 Player 2 chooses at random an encrypted from the above set. Suppose that this word is

$$(E_1(\bar{4}),E_1(\bar{5}),E_1(E_2(\bar{20}))$$

Step 4 Player 2 calculates $E_2(E_1(\bar{5}))$ and he sends it back to P_1.

Step 5 Player 1 calculates $D_1(E_2(E_1(\bar{5})))=E_2(\bar{5})$

Step 6 Both players make public their encrypted types $\mu_1(k_1^2)$ and $\mu_2(k_2^1)$.

Step 7 Player 1 calculates $\mu_2(k_2^1)^{c_1}$ and makes it public. In the same way, P_2 communicates $\mu_1(k_1^2)^{c_2}$ to P_1.

Step 8 Player 1 calculates $\gamma_1^{21}=(\mu_1(k_1^2)^{c_2}+\mu_2(k_2^1)^{c_1})^{c_1}$ and he sends it to P_2.

Step 9 Player 2 calculates $\gamma_2^{21}=(\mu_1(k_1^2)^{c_2}+\mu_2(k_2^1)^{c_1})^{c_2}$ and he makes it public.

Step 10 Player 1 calculates $E_2(\bar{5})^{\gamma_1^{21}}$ and player 2 calculates $E_1(\bar{4})^{\gamma_2^{21}}$ and they exchange these messages.

Step 11 Each player deciphers its own message, obtaining $\bar{4}^{\gamma_2^{21}}$ (the first player) and $\bar{5}^{\gamma_1^{21}}$ (the second one).

Step 12 Since $\bar{4}^{\gamma_2^{21}}\in A_1^2$ player 1 plays a_1^2 and player 2 plays a_2^1 because $\bar{5}^{\gamma_1^{21}}\in A_2^1$.

Notice that, by obeying this protocol, players replicate the probability distributions associated to the initial canonical communication equilibrium. Hence, each type of player 1 will just get an interim payoff of 5.5,

the same one than by using the original communication device. Lehrer and Sorin (1996) show how this communication equilibrium can also be replicated by using a deterministic correlated device whose outputs are public (mediated communication). However, they use jointly controlled lotteries instead of plain conversation schemes between players.

Forges' example reconsidered.

Let us reconsider next Forges' example. To emulate the communication equilibrium we define as above a correlation device *cd* such that:

(a) *cd* selects the prime number 43.

(b) *cd* chooses a two-letter words in $GF(43) \times GF(43)$, say $V = \{(\bar{2}, \bar{3})\}$

(c) *cd* selects the functions μ_h given by $\mu_1(k_1^1) = m_1 \in GF(43)$, $\mu_1(k_1^2) = m_2 \in GF(43)$, $\mu_2(k_2^1) = n_1 \in GF(43)$ and $\mu_2(k_2^2 1) = n_2 \in GF(43)$ with m_1, m_2, n_1 and n_2 four distinct elements of $GF(43)$ and satisfying the required properties as above.

(d) *cd* defines partitions of the sets of messages:

i. $V_{(a_1^1,a_2^1),(k_1^1,k_2^1)} = \{(\bar{2}, \bar{3})\}$
ii. $V_{(a_1^2,a_2^2),(k_1^1,k_2^1)} = \emptyset$
iii. $V_{(a_1^1,a_2^1),(k_1^2,k_2^1)} = \{(\bar{2}, \bar{3})\}$
iv. $V_{(a_1^2,a_2^2),(k_1^2,k_2^1)} = \emptyset$
v. $V_{(a_1^1,a_2^1),(k_1^1,k_2^2)} = \{(\bar{2}, \bar{3})\}$
vi. $V_{(a_1^2,a_2^2),(k_1^1,k_2^2)} = \emptyset$
vii. $V_{(a_1^1,a_2^1),(k_1^2,k_2^2)} = \emptyset$
viii. $V_{(a_1^2,a_2^2),(k_1^2,k_2^2)} = \{(\bar{2}, \bar{3})\}$

(e) *cd* defines the decision sets

i. $A_1^1 = \{\bar{2}^{\gamma_2^{11}}, \bar{2}^{\gamma_2^{12}}, \bar{2}^{\gamma_2^{21}}\}$
ii. $A_1^2 = \{\bar{2}^{\gamma_2^{22}}\}$
iii. $A_2^1 = \{\bar{3}^{\gamma_1^{11}}, \bar{3}^{\gamma_1^{12}}, \bar{3}^{\gamma_1^{21}}\}$
iv. $A_2^1 = \{\bar{3}^{\gamma_1^{22}}\}$

where $\gamma_h^{lm} = (\mu_1(k_1^l)^{c_2} + \mu_2(k_2^m)^{c_1})^{c_h}$, with $l = 1, 2$ and $m = 1, 2$.

(f) *cd* send the elements p, V, μ_h, c_h, A_h^1 and A_h^2 to player h.

Next, the conversation phase starts. Suppose that nature has chosen the types k_1^1 and k_2^2 and that players have selected E_h and D_h. The plain conversation between the players consists of[24]:

Step 1 Player 2 adds the control letter to every word in V. Hence, he builds up a new set given by:

$$\{(\bar{2}, \bar{3}, E_2(\bar{6}))\}$$

and he sends this set to P_1.

Step 2 Player 1 codifies the three letter word of the above set $\{(E_1(\bar{2}), E_1(\bar{3}), E_1(E_2(\bar{6})$ and he sends the encrypted word back to player 2.

Step 3 Player 2 chooses the only word in this set.

Step 4 Player 2 calculates $E_2(E_1(\bar{3}))$ and sends it to player 1.

Step 5 Player 1 calculates $D_1(E_2(E_1(\bar{3}))) = E_2(\bar{3})$

Step 6 Both player make public their encrypted type $\mu_1(k_1^1) = m_1$ and $\mu_2(k_2^2) = n_2$.

Step 7 Player 1 calculates $\mu_2(k_2^2)^{c_1}$ and makes it public. In the same way, P_2 communicates $\mu_1(k_1^1)^{c_2}$ to P_1.

Step 8 Player 1 calculates $\gamma_1^{12} = (\mu_1(k_1^1)^{c_2} + \mu_2(k_2^2)^{c_1})^{c_1}$ and sends it back to P_2.

Step 9 Player 2 calculates $\gamma_2^{12} = (\mu_1(k_1^1)^{c_2} + \mu_2(k_2^2)^{c_1})^{c_2}$ and makes it public.

Step 10 Player 1 calculates $E_2(\bar{3})^{\gamma_1^{12}}$ and player 2 calculates $E_1(\bar{2})^{\gamma_2^{12}}$ and exchange these messages.

Step 11 Each player deciphers its own message, obtaining $\bar{2}^{\gamma_2^{12}}$ (the first player) and $\bar{3}^{\gamma_1^{12}}$ (the second one).

Step 12 Since $(\bar{2})^{\gamma_2^{12}} \in A_1^1$ player 1 plays a_1^1 and player 2 plays a_2^1 because $(\bar{3})^{\gamma_1^{12}} \in A_2^1$.

[24]Since the communication equilibrium in this example is deterministic, the steps of the protocol to emulate the associated distribution are trivial and can be removed. We maintain them to show the relationships between the theoretical construction and the example.

The problem pointed out by Forges, i. e. the impossibility of simultaneous signaling and decision making, is avoidable with our protocol. This fact is a direct consequence of the properties of γ^{lm}:

(a) Firstly, γ^{lm} is calculated from the declared types of both players $\mu_1(k_1^l)$ and $\mu_2(k_2^m)$. Once a player has announced $\mu_h(k_h^l)$, he is not able to determine $\gamma^{l'm}$ for a different type $k_h^{l'}$.

(b) Secondly, both the transmission of information and the decision making depend on γ^{lm}.

Hence, it is not possible that a player can split both processes and act as if he were of a different type in each, signaling and decision making, phase. With protocols without this property this separation is, of course, possible[25].

Example 1 (continuation: deviations' analysis).

We have shown in example 1 that, by faithfully obeying our communication scheme, player 1 (of any type) reaches the same payoff than by using the original communication device. We will show here that the best strategy of player 1 is to be honest and follow the protocol, i. e. no unilateral deviation can improve his expected payoff.

Let us assume firstly that P_1 of type k_1^2 mixes all his feasible deviations:

(a) He declares to be of type k_1^1 at step 6. Hence he induces a probability distribution on actions Δ_1^{21} instead of that of 'sincere revelation' Δ_1^{22}. This new distribution is given by:

[25]Suppose, for instance, that we take away step 7 from our communication protocol. Moreover, assume that every player calculates its own exponent γ in the following way: $\gamma_1^{lm} = \mu_1(k_1^h)\mu_2(k_2^m)^{c_1}$ and $\gamma_2^{lm} = \mu_1(k_1^h)^{c_2}\mu_2(k_2^m)$. Then player 1 of type k_1^2 could declare $\mu_1(k_1^2)$ at step 6 but would send the message $E_2(\alpha_2^\star)^{\gamma_1^{1m}}$ at step 10. By deviating, player 1 gets the two goals pointed up by Forges:

(a) At step 10, P_1 receives $(\alpha_1^\star)^{\gamma_1^{2m}}$. Hence, he interprets this message as being of type k_1^2 and he learns player 2's type.

(b) But, at step 10, P_2 receives $(\alpha_2^\star)^{\gamma_1^{1m}}$. In this case, player 2 'learns' that P_1 is of type k_1^1 and he is induced to play a_2^1.

$$\Delta_1^{21} = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & 0 \end{pmatrix}$$

(b) He deviates at steps 8 or 10, changing the above distribution to the new $\bar{\Delta}_1^{21}$.

Our goal is to calculate now this last distribution. By deviating at steps 8 or 10, P_1 sends a message $E_2(\bar{\alpha}_2) \neq E_2(\bar{5}^{\gamma_1^{11}})$. Since player 1 has no control on the process, $\bar{\alpha}_2$ is taken at random uniformly on $M - \{\bar{5}^{\gamma_1^{11}}\} = GF(43) - \{\bar{0}, \bar{1}, \bar{5}^{\gamma_1^{11}}\}$. Then:

(a) P_2 will detect the deviation if and only if $\bar{\alpha}_2$ is not a valid message, i.e. $\bar{\alpha}_2 \in M - \{\bar{5}^{\gamma_1^{11}}\} - (A_2^1 \cup A_2^2 - \{\bar{5}^{\gamma_1^{11}}\})$. The probability of this situation is:

$$prob(p_2 \ detects) = \frac{p-3-(n-1)}{p-3} = \frac{33}{40}$$

Let us notice that, by making p big enough, this probability could be as close to 1 as we want. Hence, the communication scheme can be designed in such a way that a deviation is detected with a probability as high as we want. The protocol is, then, quasi-sure.

Suppose that P_1 actually deviates and he is detected by P_2. Then, the latter will play according to his punishment mixed strategy ρ_2^1 given by:

$$\rho_2^1(a_2^j) = \frac{1}{2} \sum_{k_1^l \in K_1} \sum_{a_1^i \in A_1} q(a_1^i, a_2^j | k_1^l, k_2^1)$$

Hence, $\rho_2^1(a_2^1) = \rho_2^1(a_2^2) = \frac{1}{2}$.

Let ρ_1^l denote the best response of P_1 of type k_1^l against P_2's punishment strategy. It is easy to check that the biggest payoff that P_1 obtains by following ρ_1^l, π_d, is lower than that of the communication equilibrium, $\pi_c = 5.5$, regardless of his own type. For instance, if P_1 is of type k_1^1:

$$\begin{aligned}\pi_d &= \rho_1^1(a_1^1)\sum_{a_2^j\in A_2}\rho_2^1(a_2^j)u_1(a_1^1,a_2^j,k_1^1,k_2^1)\\ &+ \rho_1^1(a_1^2)\sum_{a_2^j\in A_2}\rho_2^1(a_2^j)u_1(a_1^2,a_2^j,k_1^1,k_2^1)\\ &= \rho_1^1(a_1^1)4.5+\rho_1^1(a_1^2)3.5\leq 5.5=\pi_c\end{aligned}$$

Since the same holds if P_1 is of type k_1^2, then $\pi_d\leq\pi_c$.

(b) P_2 will not detect the deviation if and only if $\bar{\alpha}_2$ is a valid message, i.e. $\bar{\alpha}_2\in A_2^1\cup A_2^2-\{\bar{5}^{\gamma_1^{11}}\}$. The probability of this situation is:

$$prob(p_2\ does\ not\ detect)=\frac{n-1}{p-3}=\frac{7}{40}$$

Assume now that P_1 has deviated and he has not been detected. Hence, $\bar{\alpha}_2$ has been chosen at random uniformly on $(A_2^1-\{\bar{5}^{\gamma_1^{11}}\})\cup A_2^2$. Then:

(a) $prob(P_2\ will\ play\ a_2^1)=prob(\bar{\alpha}_2\in A_2^1-\{\bar{5}^{\gamma_1^{11}}\})=\frac{3}{7}$

(b) $prob(P_2\ will\ play\ a_2^2)=prob(\bar{\alpha}_2\in A_2^2)=\frac{4}{7}$

Let us notice that P_1 does not know that $\bar{5}^{\gamma_1^{11}}$ is the message chosen by the protocol. He only knows the codified message $E_2(\bar{5}^{\gamma_1^{11}})$ and he is not able to decipher it. Hence, his knowledge about the behavior of P_2 is not as precise as above. To update its information, P_1 only knows the probability with which any message is suggested by the protocol, given that he is of type k_1^2 and that he has claimed being of type k_1^1 at step 6. This knowledge is resumed in the distribution Δ_1^{21}. Denote by α_2 the message suggested by the protocol and by $\bar{\Delta}_1^{21}(k_2^m,a_1^i,a_2^j)$ the probability distribution over $K_2\times A_1\times A_2$ which collects the knowledge of P_1 about the output of the communication scheme under the deviation. Hence,

$$\begin{aligned}\bar{\Delta}_1^{21}(a_2^1) &= prob(\alpha_2\in A_2^1)\ prob(P_2\ will\ play\ a_2^1|\alpha_2\in\ A_2^1)\\ &+ prob(\alpha_2\in A_2^2)\ prob(P_2\ will\ play\ a_2^1|\alpha_2\in\ A_2^2)\\ &= \Delta_1^{21}(a_2^1)\frac{3}{7}+\Delta_1^{21}(a_2^2)\frac{4}{7}=\frac{13}{28}\end{aligned}$$

and then $\bar{\Delta}_1^{21}(a_2^2) = \frac{15}{28}$.

Before making his decision, player 1 gets some additional information: at step 11, he receives his suggestion to play. In our example, the message received is $\bar{4}^{\gamma_2^{11}} \in A_1^1$. Hence, P_1 knows that he is invited to play a_1^1 and that he is able to update his information in the following way:

$$\begin{aligned}\bar{\Delta}_1^{21}(a_2^1|a_1^1) &= prob(\alpha_2 \in A_2^1|a_1^1)\ prob(P_2\ will\ play a_2^1|\alpha_2 \in\ A_2^1, a_1^1) \\ &+ prob(\alpha_2 \in A_2^2|a_1^1)\ prob(P_2\ will\ play a_2^1|\alpha_2 \in\ A_2^2, a_1^1)) \\ &= \Delta_1^{21}(a_2^1|a_1^1)\frac{3}{7} + \Delta_1^{21}(a_2^2|a_1^1)\frac{4}{7} = \frac{10}{21}\end{aligned}$$

and then $\bar{\Delta}_1^{21}(a_2^2|a_1^1) = \frac{11}{21}$. In the same way, he is able to calculate $\bar{\Delta}_1^{21}(a_2^1|a_1^2) = \frac{3}{7}$ and $\bar{\Delta}_1^{21}(a_2^2|a_1^2) = \frac{4}{7}$.

Player 1 has now all the information to calculate his optimal action under each suggestion from the protocol. Let us remark that, in this example, player 2 has only one feasible type. Hence, we do not need to consider P_2's types to solve P_1's optimization decision problems.

If a_1^1 is suggested , the optimal action of P_1, denoted by $\bar{a}_1^1$ is given by:

$$\bar{a}_1^1 = arg\ max_{a_1 \in A_1} \sum_{j=1,2} (\bar{\Delta}_1^{21}(a_2^j|a_1^1) u_1(k_1^2, k_2^1, a_1, a_2^j)$$

Just by checking both possible values of $\bar{a}_1^1$ we obtain that $\bar{a}_1^1 = a_1^2$ and the expected payoff in this case is $\frac{32}{7}$.

If a_1^2 is suggested , the optimal action of P_1, denoted by $\bar{a}_1^2$ is given by:

$$\bar{a}_1^2 = arg\ max_{a_1 \in A_1} \sum_{j=1,2} (\bar{\Delta}_1^{21}(a_2^j|a_1^2) u_1(k_1^2, k_2^1, a_1, a_2^j)$$

Just by checking both possible values of $\bar{a}_1^2$ we obtain that $\bar{a}_1^2 = a_1^2$ and the expected payoff in this case is given by $\frac{33}{7}$.

Before step 6, when player 1 makes his first decision about cheating or not, his expected payoff, π_{nd}, is given by $\pi_{nd} = \Delta(a_1^1)\frac{32}{7}+\Delta(a_1^2)\frac{33}{7} = \frac{129}{28}$. But this expected payoff is less than 5.5, the payoff that he could obtain by faithfully following the protocol. Hence, player 1 has no incentive to deviate from the protocol at step 6.

Similarly, it can be checked that the expected payoff obtained by honestly revealing type k_1^2 at step 6 and by deviating at steps 8 or 10 is given by $\pi_{nd} = \frac{123}{28}$. This payoff is also lower than that of the original communication equilibrium, i. e. $\pi_{nd} \leq \pi_c$.

Hence, we have shown that no unilateral deviation can increase player 1's profits and the communication scheme is, in this example, self-enforcing. In the following sections we will prove that this is a general property of our communication protocol.

Analysis of deviations.

We classify the deviations from the protocol in two main groups. Firstly, we can find deviations, such as declaring false types or choosing non suggested actions given an information set, with a strong strategic meaning. Secondly, there are other deviations which have only random effects: the deviating player puts some noise into the system, with no control on the changes in the players' knowledge states that he is producing. These deviations are denoted as *deviations from the rules*, and they may take place at steps[26] 8 or 10, by changing either the right value of the exponent of γ_h^{lm} or the right message to be sent at step 10. Clearly, both deviations have the same effect[27]: the non-cheating player, say $P_{h'}$, will receive a message $E_{h'}(\bar{\alpha}_{h'})$ in $M = GF(p) - \{\bar{0}, \bar{1}\}$ distinct from $E_{h'}(\alpha^{\star}_{h'})^{\gamma_h^{lm}}$. Afterwards, two situations may take place:

(a) If $(\bar{\alpha}_{h'}) \in M - \cup_{j=1}^{t} A_2^j$, $P_{h'}$ will realize that a deviation from the rules has happened. Hence,

$$prob(P_{h'} \; detects \; a \; deviation \; from \; the \; rules) =$$

[26] Deviations at step 7 are not considered, since they are dominated by faithfully playing.
[27] Since exponential functions on a $GF(p)$ induce bijective maps.

$$\frac{card(M) - 1 - (card(\cup_{j=1}^{t} A_2^j) - 1)}{card(M) - 1} = \frac{p - n}{p - 3}$$

where $n = card(\cup_{j=1}^{t} A_2^j)$. Let us remark that, for any $\varepsilon > 0$ and for any size of the decision sets A_2^j, we can take a prime number p such that

$$prob(P_{h'} \text{ detects a deviation from the rules}) < 1 - \varepsilon$$

Hence, we have that

Proposition 1 *The communication protocol defined above is quasi-sure, i. e., $\forall \varepsilon > 0$, any deviation from the rules is detected by the non-cheating player with probability $1 - \varepsilon$.*

(b) If $\bar{\alpha}_{h'} \in \cup_{j=1}^{t} A_2^j - \{(\alpha_{h'}^{\star})^{\gamma_h^{lm}}\}$, $P_{h'}$ takes the false message as a valid one. Hence, his information set will change and he will made a different choice of the action to play. Let us denote by $\bar{\Delta}_h^{ll'}$ the probability distribution over $K_{h'} \times A_h \times A_{h'}$ which resumes the information of the cheating player who has deviated both strategically (by announcing that he is of type $k_h^{l'}$ while he is in fact of type k_h^l) and from the rules, and this latter deviation has not been detected, i.e., $\bar{\Delta}_h^{ll'}(k_{h'}^m, a_h^i, a_{h'}^j) = \pi(k_{h'}^m | k_h^l) q(a_h^i, a_{h'}^j | k_h^{l'}, k_{h'}^m)$ resumes the information of P_h about the probability of player h' being of type $k_{h'}^m$, the action of $P_{h'}$ being $a_{h'}^j$ and his own suggested action being a_h^i, when P_1 is of type k_1^l and he pretends to be $k_1^{l'}$.

We establish next the properties of the distributions $\bar{\Delta}_h^{ll'}$. To undertake our analysis, assume that player 1 has deviated from the rules and player 2 has not detected him.

Lemma 1 *If player 1 deviates and player 2 does not detect him, actions will be suggested with the following probabilities:*

(a) $\bar{\Delta}_1^{ll'}(a_1^i) = \Delta_1^{ll'}(a_1^i)$, $\forall a_1^i \in A_1$.

(b) $\bar{\Delta}_1^{ll'}(a_2^j) = \frac{card(A_2^j) - \Delta_1^{ll'}(a_2^j)}{n-1}$, $\forall a_2^j \in A_2$ *where* $n = card(\cup_{j=1}^{t} A_2^j)$.

Proof: The first assertion holds since player 2 is faithfully following the protocol.

In order to prove 2, let us remark that, since a deviation from the rules has taken place, P_2 is receiving a message $\bar{\alpha}_{h'}$ in some A_2^j different from $(\alpha_{h'}^\star)^{\gamma_h^{lm}}$. This message will be in A_2^u with a probability $\Delta_1^{ll'}(a_2^u)$. Then, we know that $\bar{\alpha}_{h'}$ will be:

(a) Either any of the $Card(A_2^u) - 1$ elements of $A_2^u - \{(\alpha_{h'}^\star)^{\gamma_h^{lm}}\}$

(b) or any of the $Card(A_2^{u'})$ elements of $A_2^{u'}$, $\forall u' \neq u$.

with the same probability. Hence,

$$\begin{aligned}\bar{\Delta}_1^{ll'}(a_2^j) &= \sum_{u=1,u\neq j}^{t} \Delta_1^{ll'}(a_2^u)\frac{Card(A_2^j)}{n-1} + \Delta_1^{ll'}(a_2^j)\frac{Card(A_2^j)-1}{n-1} \\ &= \frac{Card(A_2^j) - \Delta_1^{ll'}(a_2^j)}{n-1}\end{aligned}$$

□

Moreover, player 1's information on player 2's type is the same whether or not P_1 is following the protocol. Hence,

Lemma 2 *Assume that player 1 deviates and that he is not detected by player 2. Then, $\forall k_2^m \in K_2$, $a_1^i \in A_1$ and $k_1^l, k_1^{l'} \in K_1$, the information of the cheating player about the type of the other is given by:*

(a) $\bar{\Delta}_1^{ll'}(k_2^m|a_1^i) = \Delta_1^{ll'}(k_2^m|a_1^i)$

(b) $\bar{\Delta}_1^{ll'}(k_2^m, a_1^i) = \Delta_1^{ll'}(k_2^m, a_1^i)$

Finally, let us analyze how player 1's knowledge about player 2's action is updated under deviations from the rules. As we said above, when P_1 deviates and he is not detected, he generates a new distribution over actions and players' types

Lemma 3 *Assume that player 1 deviates and that he is not detected by player 2. Then,* $\forall k_1^l, k_1^{l'} \in K_1,\ k_2^m \in K_2,\ a_1^i \in A_1$ *and* $a_2^j \in A_2$, *the information of the cheating player about the action that is suggested to the other one is given by:*

(a) $\bar{\Delta}_1^{ll'}(a_2^j|a_1^i) = \frac{card(A_2^j) - \Delta_1^{ll'}(a_2^j|a_1^i)}{n-1}$

(b) $\bar{\Delta}_1^{ll'}(a_2^j|a_1^i, k_2^m) = \frac{card(A_2^j) - \Delta_1^{ll'}(a_2^j|a_1^i, k_2^m)}{n-1}$
where $n = card(\cup_{u=1}^{t} A_2^u)$.

Proof: The sketch of the proof is similar to the one above. P_2 receives a false message $\bar{\alpha}_{h'}$ in some A_2^u different from $(\alpha_{h'}^{\star})^{\gamma_h^{lm}}$. This message will be in A_2^u with probability $\Delta_1^{ll'}(a_2^u 1^i)$. Then, $\bar{\alpha}_{h'}$ will be:

(a) Either any of the $Card(A_2^u) - 1$ elements of $A_2^u - \{(\alpha_{h'}^{\star})^{\gamma_h^{lm}}\}$

(b) or any of the $Card(A_2^{u'})$ elements of $A_2^{u'}$, $\forall u' \neq u$.

with the same probability. Hence,

$$\begin{aligned}
\bar{\Delta}_1^{ll'}(a_2^j|a_1^i) &= \sum_{u=1, u\neq j}^{t} \Delta_1^{ll'}(a_2^u|a_1^i)\frac{Card(A_2^j)}{n-1} + \Delta_1^{ll'}(a_2^j|a_1^i)\frac{Card(A_2^j)-1}{n-1} \\
&= \frac{Card(A_2^j) - \Delta_1^{ll'}(a_2^j|a_1^i)}{n-1}
\end{aligned}$$

The second assertion is proved in the same way by just conditioning every probability on k_2^m as well.

□

From correlation to Nash equilibrium.

Our main result states that a communication device can be substituted by unmediated communication scheme in any two-player game of incomplete information and rational parameters. But the theorem just shows the power of plain conversation as an *information transmission mechanism*: all solution in $T(G)$ can be achieved as correlated equilibrium payoffs of the single game G extended by a universal scheme of

unmediated communication. However, correlated equilibrium strategies may need the help of a correlation device, which may a priori depend on the parameters of the game. Thus, in order to show the power of plain conversation as a *coordination mechanism* we need that the players generate by pre-play unmediated communication the same effect than a correlation device, i. e. that they can get rid of the correlated device. We can show that under appropriate assumptions on G, a similar result to that of our theorem holds for the set of correlated equilibrium payoffs of G: they are achieved as Nash equilibrium payoffs of G extended by a universal mechanism of pre-play unmediated communication. To generate this internal correlation we use the result of Urbano and Vila (1997), which we state for completeness:

Proposition 2 (Urbano and Vila, 1997) *Let Γ be a two-player game with complete information and rational payoffs. Let $C(\Gamma)$ be the set of correlated equilibrium payoffs of Γ. Then, every payoff in $C(\Gamma)$ is achievable as a Nash equilibrium payoff of the game extended by a universal mechanism of pre-play unmediated communication. The equilibrium strategies use only finite sets of messages.*

By using this proposition, the correlation device of our unmediated communication scheme can also be removed by a second unmediated conversation scheme. The idea is to apply the above construction to the game obtained by adding to G the universal mechanism of interim pre-play conversation described in the main result. This yields another universal mechanism of unmediated communication, which takes place before the players learn their types in G: ex-ante pre-play communication. The purpose of this earlier phase is to generate internal correlation and thus to remove the role of the correlation device. We can then establish:

Proposition 3 *Let G be a two-player game with incomplete information and rational parameters. Let $T(G)$ the set of communication equilibrium payoffs of G. Then, every payoff in $T(G)$ is achievable as a Nash equilibrium payoff of the game extended by a universal mechanism consisting on two phases of (ex-ante and interim) pre-play unmediated communication. Moreover, the equilibrium strategies only use finite sets of messages.*

Proof: The proof is straightforward. Let us denote by $EC\Gamma$ the game where the players first talk according to EC and then they play Γ. Let ic be the universal mechanism of interim pre-play communication described in our main result and let icG be the extension of G where the players talk according to ic just before making decisions. The theorem states that $T(G) \subseteq C(icG)$, and thus $T(G) = C(icG)$. Now suppose that G has rational payoffs functions and probability distributions on Q, then by applying our result to G and that of Proposition 2 (Urbano and Vila, 1997) to $\Gamma = icG$, we obtain $T(G) = N(ECicG)$, where N stands for the Nash equilibrium payoffs and EC is the ex-ante unmediated communication protocol of Proposition 2.

□

Proof of the main result.

We prove next that our communication protocol is self-enforcing, i. e. there exists no unilateral profitable deviation. We split this proof into to steps. The first one concerns with the proof of the following lemma:

Lemma 4 *Assume, without loss of generality that player 2's types are equally likely (i. e. $\pi(k_2^m) = \pi(k_2^{m'})$, for all $m, m' = 1, .., r$)*[28]*. Then, the space of valid messages V can be taken large enough to guarantee that there is no undetectable profitable deviation from the unmediated communication protocol, i. e.*

$$\sum_{i=1}^{s} \Delta_1^{ll}(a_1^i) \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_1^{ll}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, a_1^i, a_2^j) \geq$$

$$\sum_{i=1}^{s} \bar{\Delta}_1^{ll'}(a_1^i) \sum_{m=1}^{r} \sum_{j=1}^{t} \bar{\Delta}_1^{ll'}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j)$$

[28] If this were not the case, the rationality of the probabilities $\pi(k_2^j)$ would allow us to add new types (with the same induced payoffs) until each type had equal probability to be chosen by nature. Therefore, we can make the assumption of equal likelihood of types without loss of generality.

where

$$\bar{a}_1^i = arg\ max_{a_1 \in A_1} \sum_{m=1}^{r} \sum_{j=1}^{t} \bar{\Delta}_1^{ll'}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, a_1, a_2^j)$$

Proof: Denote by OB the payoff that P_1 obtains by obeying the protocol and by $D(n)$ the maximum expected payoff by deviating. Let us make explicit the meaning of the parameter n. As we have pointed out above, $n = card(\cup_{j=1}^{t} A_2^j) = card(V)$. Given a communication equilibrium, n is fixed and it is a measure of the complexity of the probability distribution supporting this equilibrium. Notice that, for such a given equilibrium, we are able to increase n as much as we want by just considering a set of valid messages $\bar{V}$ which is constructed by joining several copies of the original set V. By maintaining the proportion of assigned elements to each action of both players, all our construction remains unchanged. Hence, without loss of generality, we can assume that n is a free parameter of the problem.

We establish next the bounds of the payoffs from both obeying and deviating behavior. By using communication equilibrium distribution inequalities, we have that:

$$\begin{aligned}
OB &= \sum_{i=1}^{s} \Delta_1^{ll}(a_1^i) \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_1^{ll}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, a_1^i, a_2^j) \\
&\geq \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_1^{ll'}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, \hat{a}_1^i, a_2^j) \\
&= \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m | a_1^i) \sum_{j=1}^{t} \Delta_1^{ll'}(a_2^j | a_1^i, k_2^m) u_1(k_1^l, k_2^m, \hat{a}_1^i, a_2^j)
\end{aligned}$$

where

$$\hat{a}_1^i = arg\ max_{a_1 \in A_1} \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_1^{ll'}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, a_1, a_2^j)$$

is the action that optimizes the expected payoff of P_1 when he is of type k_1^l but he announces to be of type $k_1^{l'}$.

Consider now the profits of a deviation from the rules. Denote by $\bar{a}_1^i$ the optimal action of player 1, when he deviates (and he is not detected) and he is suggested to play a_1^i, i. e.

$$\bar{a}_1^i = arg\ max_{a_1 \in A_1} \sum_{m=1}^{r} \sum_{j=1}^{t} \bar{\Delta}_1^{ll'}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, a_1, a_2^j)$$

Hence, by the properties of $\bar{\Delta}_1^{ll'}$, we have that:

$$\begin{aligned}
D(n) &= \sum_{i=1}^{s} \bar{\Delta}_1^{ll'}(a_1^i) \sum_{m=1}^{r} \sum_{j=1}^{t} \bar{\Delta}_1^{ll'}(k_2^m, a_2^j | a_1^i) u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j) \\
&= \sum_{i=1}^{s} \bar{\Delta}_1^{ll'}(a_1^i) \sum_{m=1}^{r} \bar{\Delta}_1^{ll'}(k_2^m | a_1^i) \sum_{j=1}^{t} \bar{\Delta}_1^{ll'}(a_2^j | a_1^i, k_2^m) u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j) \\
&= \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m | a_1^i) \sum_{j=1}^{t} \frac{card(A_2^j) - \Delta_1^{ll'}(a_2^j | a_1^i, k_2^m)}{n-1} u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j) \\
&= \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m | a_1^i) \\
&\quad \sum_{j=1}^{t} (\frac{n}{n-1} \frac{card(A_2^j)}{n} - \frac{1}{n-1} \Delta_1^{ll'}(a_2^j | a_1^i, k_2^m)) u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j) \\
&= \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m | a_1^i) \\
&\quad \sum_{j=1}^{t} (\frac{n}{n-1} \Delta_1^{ll'}(a_2^j) - \frac{1}{n-1} \Delta_1^{ll'}(a_2^j | a_1^i, k_2^m)) u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j)
\end{aligned}$$

where the identity $\frac{card(A_2^j)}{n} = q(a_2^j) = \Delta_1^{ll'}(a_2^j)$ holds because player 2's types are equally likely (i. e. $\pi(k_2^m) = \pi(k_2^{m'})$, for all $m, m' = 1, .., r$).

Denote by $D = \lim_{n\to\infty} D(n)$ the limit payoff. Hence,

$$\begin{aligned} D &= \lim_{n\to\infty} D(n) \\ &= \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m|a_1^i) \sum_{j=1}^{t} q(a_2^j) u_1(k_1^l, k_2^m, \bar{a}_1^i, a_2^j) \end{aligned}$$

Let us remark that, in the limit, payoffs can be improved by playing $\tilde{a}_1^i$ given by:

$$\tilde{a}_1^i = arg\ max_{a_1\in A_1} \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m|a_1^i) \sum_{j=1}^{t} q(a_2^j) u_1(k_1^l, k_2^m, a_1, a_2^j)$$

and we have that

$$D \leq \sum_{i=1}^{s} \Delta_1^{ll'}(a_1^i) \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m|a_1^i) \sum_{j=1}^{t} \Delta_1^{ll'}(a_2^j) u_1(k_1^l, k_2^m, \tilde{a}_1^i, a_2^j)$$

The two above optimization problems

$$\hat{a}_1^i = arg\ max_{a_1\in A_1} \sum_{m=1}^{r} \sum_{j=1}^{t} \Delta_1^{ll'}(k_2^m, a_2^j|a_1^i) u_1(k_1^l, k_2^m, a_1, a_2^j)$$

$$\tilde{a}_1^i = arg\ max_{a_1\in A_1} \sum_{m=1}^{r} \Delta_1^{ll'}(k_2^m|a_1^i) \sum_{j=1}^{t} \Delta_1^{ll'}(a_2^j) u_1(k_1^l, k_2^m, a_1, a_2^j)$$

are almost identical. The only difference between them is that P_1 has in the first problem more information to calculate his optimal action. Since he can always disregard (or not use) his information, the solution to the second problem can never be better than the solution to the first one and

$$\sum_{i=1}^{s}\Delta_1^{ll'}(a_1^i)\sum_{m=1}^{r}\Delta_1^{ll'}(k_2^m|a_1^i)\sum_{j=1}^{t}\Delta_1^{ll'}(a_2^j|a_1^i,k_2^m)u_1(k_1^l,k_2^m,\hat{a}_1^i,a_2^j)$$

$$\geq \sum_{i=1}^{s}\Delta_1^{ll'}(a_1^i)\sum_{m=1}^{r}\Delta_1^{ll'}(k_2^m|a_1^i)\sum_{j=1}^{t}q(a_2^j)u_1(k_1^l,k_2^m,\bar{a}_1^i,a_2^j)$$

Joining all these inequalities, we have that $OB \geq D = \lim_{n\to\infty} D(n)$. Then, there exists n_0 such that $OB \geq D(n_0)$. Hence, taking V big enough (i.e. $card(V) \geq n_0$), there is no undetected unilateral profitable deviation and the proposition holds.

□

Proposition 4 *The communication protocol is self-enforcing*

Proof: To establish this result we need to prove that the biggest payoff that P_1 can get by deviating is lower than the correlated equilibrium payoff. This 'highest payoff from deviating', π, satisfies that: $\pi \leq \varepsilon\pi_d + (1-\varepsilon)\pi_{nd}$, where π_d and π_{nd} are the biggest payoffs that P_1 can obtain when P_2 detects and does not detect, respectively, his deviation.

Denote by π_c the correlated equilibrium payoff. Since the above lemma holds, we have that $\pi_{nd} \leq \pi_c$. Hence, it only suffices to show that $\pi_d \leq \pi_c$.

Assume that $\rho_1^l(a_1^i)$, is the best response (mixed strategy) of P_1 of type k_1^l to player 2's punishment strategy and recall that $K_1 = \{k_1^1,...,k_1^v\}$, $K_2 = \{k_2^1,...,k_2^r\}$, $A_1 = \{a_1^1,...,a_1^s\}$ and $A_2 = \{a_2^1,...,a_2^t\}$. We have that:

$$\pi_d = \sum_{m=1}^{r}\pi(k_2^m|k_1^l)\sum_{i=1}^{s}\rho_1^l(a_1^i)\sum_{j=1}^{t}\rho_2^m(a_2^j)u_1(a_1^i,a_2^j,k_1^l,k_2^m)$$

$$= \sum_{i=1}^{s}\rho_1^l(a_1^i)\frac{1}{|K_1|}\sum_{l'=1}^{v}\sum_{m=1}^{r}\sum_{j=1}^{t}\sum_{i'=1}^{s}\pi(k_2^m|k_1^l)q(a_1^{i'},a_2^j|k_1^{l'},k_2^m)u_1(a_1^i,a_2^j|k_1^l,k_2^m)$$

$$= \sum_{i=1}^{s} \rho_1^l(a_1^i) \frac{1}{|K_1|} \sum_{l'=1}^{v} \sum_{m=1}^{r} \sum_{j=1}^{t} \sum_{i'=1}^{s} \Delta_1^{ll'}(k_2^m, a_1^{i'}, a_2^j) u_1(a_1^i, a_2^j | k_1^l, k_2^m)$$

Since we are dealing with a communication equilibrium distribution,

$$\sum_{m=1}^{r} \sum_{j=1}^{t} \sum_{i'=1}^{s} \Delta_1^{ll'}(k_2^m, a_1^{i'}, a_2^j) u_1(a_1^i, a_2^j | k_1^l, k_2^m) \leq$$

$$\sum_{m=1}^{r} \sum_{j=1}^{t} \sum_{i'=1}^{s} \Delta_1^{ll}(k_2^m, a_1^{i'}, a_2^j) u_1(a_1^{i'}, a_2^j | k_1^l, k_2^m) = \pi_c$$

Hence,

$$\pi_d \leq \sum_{i=1}^{s} \rho_1^l(a_1^i) \frac{1}{|K_1|} \sum_{l'=1}^{v} \pi_c = \pi_c$$

and the proposition holds.

□

Proof of the main result.

A straight consequence of the above proposition is that our main result holds for every communication equilibrium with a Q - evaluated associated probability distribution. To extend this result to R - evaluated distributions, although under the assumption that the original game has rational parameters, we can apply the same construction than Forges (1990) and Urbano and Vila (1997) : any arbitrary R-evaluated distribution is a convex combination of a finite number of Q-evaluated distribution (the vertices of the convex polyhedron of communication equilibrium distribution). Hence, the payoff associated to the real distribution can be achieved by two phases of plain conversation. In the first step a vertex is selected depending on the convex coordinates of the R- evaluated distribution and in the second step our protocol provides

the payoff associated to the Q-evaluated distribution corresponding to the vertex previously selected (See Forges (1990) for details) [29].

Concluding remarks.

We have shown in this paper the role of unmediated communication as both an information transmission and a coordination device for the class of two-player incomplete information games. This question was left open by Forges (1990) for the correlated equilibrium solution concept and by Barany (1992) for the Nash equilibrium one.

Let us relate our findings to the previous cases treated in the literature. As it was said above, satisfactory results were available for first, all games of incomplete information with at least four players (Forges, 1990) and second, for games of information transmission[30] with independent senders (Forges, 1988). For three person games of incomplete information the above result extend once the requirement of finite message sets is relaxed. Hence, the only open question here concerns the finiteness of the sets of messages.

However, although no results were available for general two-player games of incomplete information under unmediated talk, some answers have been given for specific games. Thus, for two-person Sealed Bid Double Auction games, Matthews and Postlewaite (1989) proved that the set of Bayesian-Nash equilibrium outcomes of the unmediated communication-

[29] The jointly controlled lottery of this proof can also be generated by using our communication protocol. Hence, P_1 and P_2 are able to choose a number in $\{0,1\}$ with the same probability by using the communication protocol built up in this paper to replicate the distribution

$$\begin{array}{cc} & \begin{array}{cc} 0 & 1 \end{array} \\ \begin{array}{c} 0 \\ 1 \end{array} & \left(\begin{array}{cc} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{array} \right) \end{array}$$

which can be understood as a correlated equilibrium of a 2×2 trivial game with null payoffs. Repeating this process we can obtain the binary codification of a concrete realization of the random variable v, which is uniformly distributed in $[0,1)$. This is an alternative construction to the one of Aumann, Maschler and Stearns (1968), used in the proof of Forges (1990).

[30] Including all two-person games of information transmission, i. e. 'sender - receiver' games.

bidding game defined by adding one round of simultaneous message exchange contains the equilibrium outcomes of all other communication-bidding games[31]. Although they do not need cryptographic tools, private values are essential in their construction.

When we apply our approach to *bilateral trading with asymmetric information* and in particular to *two-person Sealed Bid Double Auction* games, our main result states that the set of correlated equilibrium outcomes of the resulting two-stage game contains all the equilibrium outcomes that could be obtained by adding any other communication mechanism. In other words, that the set of correlated equilibrium outcomes of an unmediated communication-bidding game defined by adding several rounds of both sequential and simultaneous messages exchange would contain the equilibrium outcomes of all other communication-bidding games. Matthews and Postlewaite, proved instead that the set of Bayesian-Nash equilibrium outcomes of the double auction game preceded by one round of simultaneous message exchange, contains the equilibrium outcomes of all other communication-bidding games. Thus, their result is stronger than ours in so far as it does not rely on correlated equilibrium[32]. However, applying the scheme of our Proposition 3 to this framework produces a communication mechanism that results in a unmeditaed communication-bidding game whose set of equilibrium outcomes contains those of all other communication-bidding games, and thus our findings are the analog of those of Matthews and Postlewaite, when the exchange of messages is not simultaneous. However, since they deal with private values[33], it is not clear that both results can be properly compared. In particular, whether our approach could eliminate some of the outcomes achieved by the scheme with simultaneous exchange of messages.

[31]Their result relies on simultaneous rather than sequential message exchange and communication in their equilibria plays only a coordination role. Farrell and Gibbons (1989) were the first to consider communication in a double auction. Although their game is a special case of that of Matthews and Postlewaite, their equilibrium is a true communication equilibrium in the sense that it both transmits information and coordinates decisions.

[32]The set of correlated equilibrium outcomes of the communication-bidding game contains its Bayesian-Nash equilibrium outcomes.

[33]The value of the object to a given agent only depends on his own type.

The fact that unmediated pre-play communication enable the traders to reach a large class of outcomes is a desirable property, because it implies that the traders can dispense with the planner. However, as emphasized by Matthews and Postlewaite (1989) and Palfrey and Srivastava (1991) pre-play communication dramatically worsens the full implementation problem. Thus a *mechanism design* problem can, in a particular sense, be converted into a *equilibrium selection* problem. The next step is then to introduce particular communication equilibria[34] and check if they can be achieved through unmediated pre-play communication. This is left for future research.

References.

M. Amitai (1996): 'Cheap talk with incomplete information on both sides.' *Discussion paper 90. The Hebrew University of Jerusalem. Center for rationality and interactive decision theory.*

R. Aumann (1974): 'Subjectivity and correlation in randomized strategies.' *Journal of Mathematical Economics 1, 67-96.*

R. Aumann (1987): 'Correlated equilibrium as an expression of Bayesian rationality.' *Econometrica 55, 1-18.*

R. Aumann, M Maschler and R. E. Stearns (1968): 'Repeated games of incomplete information.' *Mathematica Inc Princeton. (Chapter IV 117 - 216). Reprinted in Aumann and Maschler 'Repeated games with incomplete information' (Chapter 5). Cambridge, MIT Press.*

R. Aumann and S. Hart (1993): 'Polite talk isn't cheap' *Mimeo.* Hebrew University of Jerusalem.

I. Barany (1992): 'Fair distribution protocols or how the players replace fortune.' *Mathematics of Operations Research 17, 327-340.*

M. Blum (1981): 'Three applications of the oblivious transfer: Coin flipping by telephone, How to exchange secrets and How to send certified electronic mail.' *Dept. EECS, Univ of California, Berkeley.*

[34]Forges (1998) introduces the *self-fulfilling equilibria*, which she shows are equivalent to veto-incentive compatible mechanisms. In the case of private values for the trading game of one seller a n potential buyers, she also demonstrates that all the communication equilibria have these properties and can be implemented by pre-play communication.

K. Chatterjee and W. Samuelson (1983): 'Bargaining under incomplete information.' *Oper. Res. 31, 835-851.*

J. Farrell (1988): 'Communication, coordination and Nash equilibrium.' *Econ. Lett. 27, 209-214.*

J. Farrell and R. Gibbons (1989): 'Cheap talk can matter in bargaining.' *JET 48, 221-237*

J. Farrell and M. Rabin (1996): 'Cheap talk.' *Journal of Economic Perspectives 10, 103-118.*

F. Forges (1986): 'An approach to communication equilibria.' *Econometrica 54, 1375-1385.*

F. Forges (1988): 'Can sunspots replace a mediator?.' *Journal of Mathematical Economics 17, 347-368.*

F. Forges (1990): 'Universal mechanisms.' *Econometrica 58, 1341-1364.*

F. Forges (1998): 'Ex-post individually rational trading mechanisms.' *Mimeo, THEMA. Universit? de Cergy-Pontoise and Institut Universitaire de France.*

O. Gossner (1997): 'Secure protocols or how communication generates correlation.' *CORE discussion paper 9792.*

O. Gossner (1998): 'Repeated games played by crytographically sophisticated players.' *Mimeo, CORE.*

T. Gresik (1991): 'Ex ante incentive efficient trading mechanism without the private value restriction.' *JET 55, 41-63.*

T. Gresik (1996): 'Incentive-efficient equilibria of two-party sealed-bid bargaining games.' *JET 68, 26-48.*

E. Lehrer (1996): 'Mediated talk.' *International Journal of Game Theory 25, 177-188.*

E. Lehrer and S. Sorin (1997): 'One shot public mediated talk.' *Games and Economic Behavior 20, 132-148.*

W. Leininger, P. Linhart and R. Radner (1989): 'Equilibria of the sealed-bid mechanism for bargaining with incomplete information.' *JET 48, 63-106.*

S. A. Matthews and A. Postlewaite (1989): 'Pre-play communication in two-person sealed-bid double auctions.' *JET 48, 238 - 263.*

R. Myerson and M. Satterthwaite (1983): 'Efficient mechanisms for bilateral trading.' *JET 29, 265 - 281.*

J. F. Mertens (1991): 'Correlated and communication equilibria.' *Game theoretic methods in general equilibrium analysis. NATO ASI Series, Vol. 77, (Chapter XV 243 - 248). Edited by J. F. Mertens and S. Sorin.*

T. Palfrey and S. Srivastava (1991): 'Efficient trading mechanisms with pre-play communication.' *JET 29, 265 - 281.*

M. Rabin (1981): 'Exchange of secrets.' *Dept. of Applied Physics, Harvard Univ. Cambridge, Mass.*

M. Rabin (1993): 'A model of pre-game communication.' *JET 63, 370-391.*

M. Satterthwaite and S. Williams (1989): 'Bilateral trade with the sealed-bid k-double auction: existence and efficiency.' *JET 48, 107 - 133.*

S. Sorin (1991): 'Implementation with plain conversation.' *Game theoretic methods in general equilibrium analysis. NATO ASI Series, Vol. 77, (Chapter XVII 261 - 268). Edited by J. F. Mertens and S. Sorin.*

A. Urbano and J. E. Vila (1997): 'Pre-play communication and coordination in two-player games.' *IVIE Working Paper WP-AD 97-26*

A. Urbano and J. E. Vila (1998): 'Unmediated communication in repeated games with imperfect monitoring.' *IVIE working paper.*